Tracking Computer Use with the Windows® Registry Dataset

NSRL
National
Software
Reference
Library

Doug White

NIST United States Department of Commerce
National Institute of Standards and Technology

Disclaimer

Trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

Statement of Disclosure

This research was funded by the National Institute of Standards and Technology Office of Law Enforcement Standards, the Department of Justice National Institute of Justice, the Federal Bureau of Investigation and the National Archives and Records Administration.

National Software Reference Library & Reference Data Set

The NSRL is conceptually three objects:

- A physical collection of software
- A database of meta-information
- A subset of the database,
  the Reference Data Set

The NSRL is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set of information.

Windows® Registry Data Set

It is possible to compile a historical list of applications based on RDS metadata and residue files.

Many methods can be used to remove application files, but these may not purge the Registry.

Examining the Registry for residue can augment a historical list of applications or provide additional context about system use.

Windows® Registry Data Set (WiReD)

The WiReD contains changes to the Registry caused by application installation, de-installation, execution or other modifying operations.

The applications are chosen from the NSRL collection, to be of interest to computer forensic examiners.

WiReD is currently an experimental prototype.

NIST is soliciting feedback from the computer forensics community to improve and extend its usefulness.

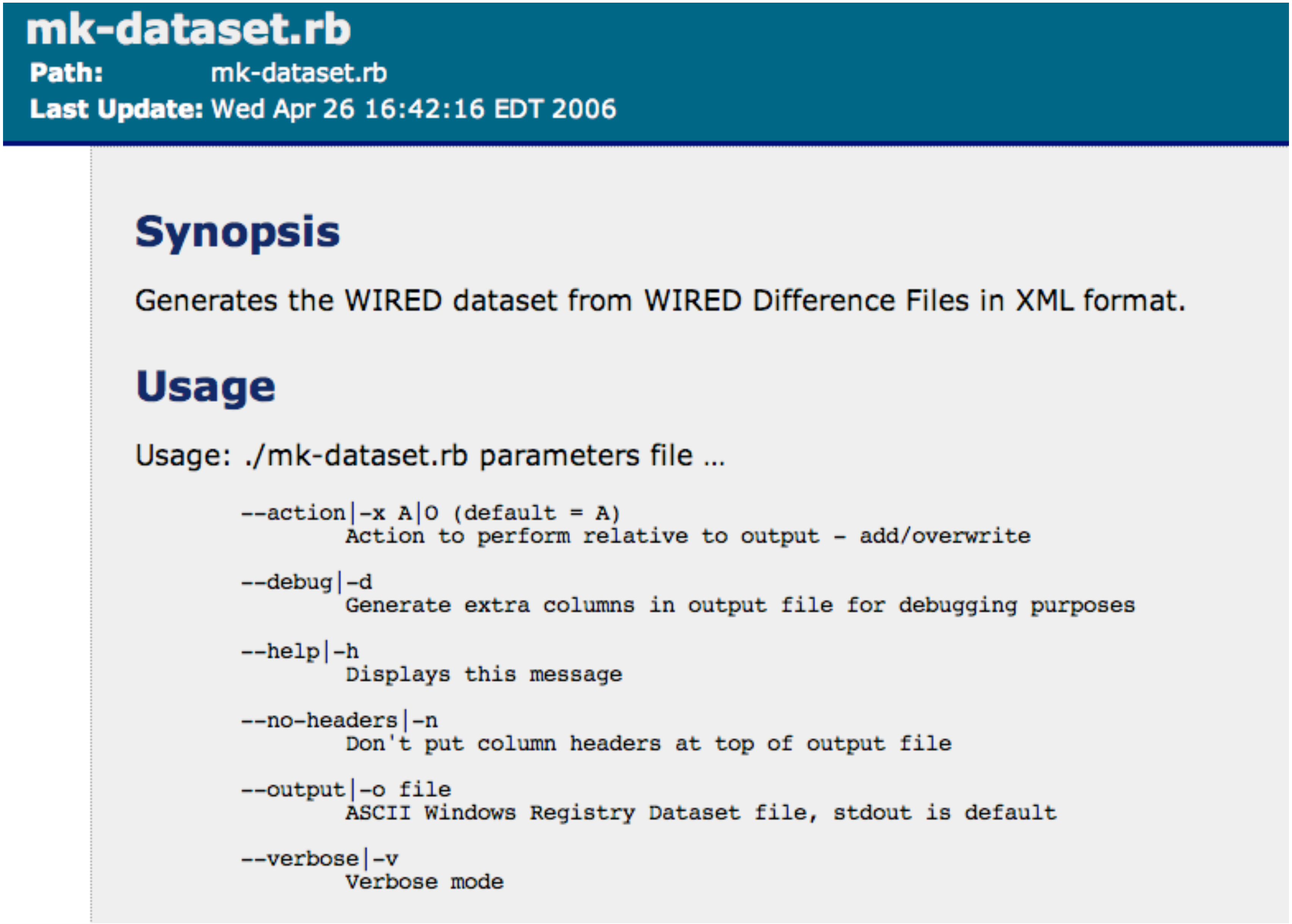
Implementation

There are currently two tools implemented:

1. mk-dataset.rb - creates the WiReD dataset from difference files generated by reg-diff.rb.
2. reg-diff.rb - generates a XML-based difference between two Microsoft RegEdit-generated Registry patch files.

The WiReD tools are currently implemented in Ruby (1.8.4) and were tested in Mac OS X 10.4 (Tiger).

The complete set of code and and a WiReD XML difference set for steganographic applications can be downloaded at http://www.nsrl.nist.gov/WIRED/WIRED-060511.iso



mk-dataset.rb

Path: mk-dataset.rb

Last Update: Wed Apr 26 16:42:16 EDT 2006

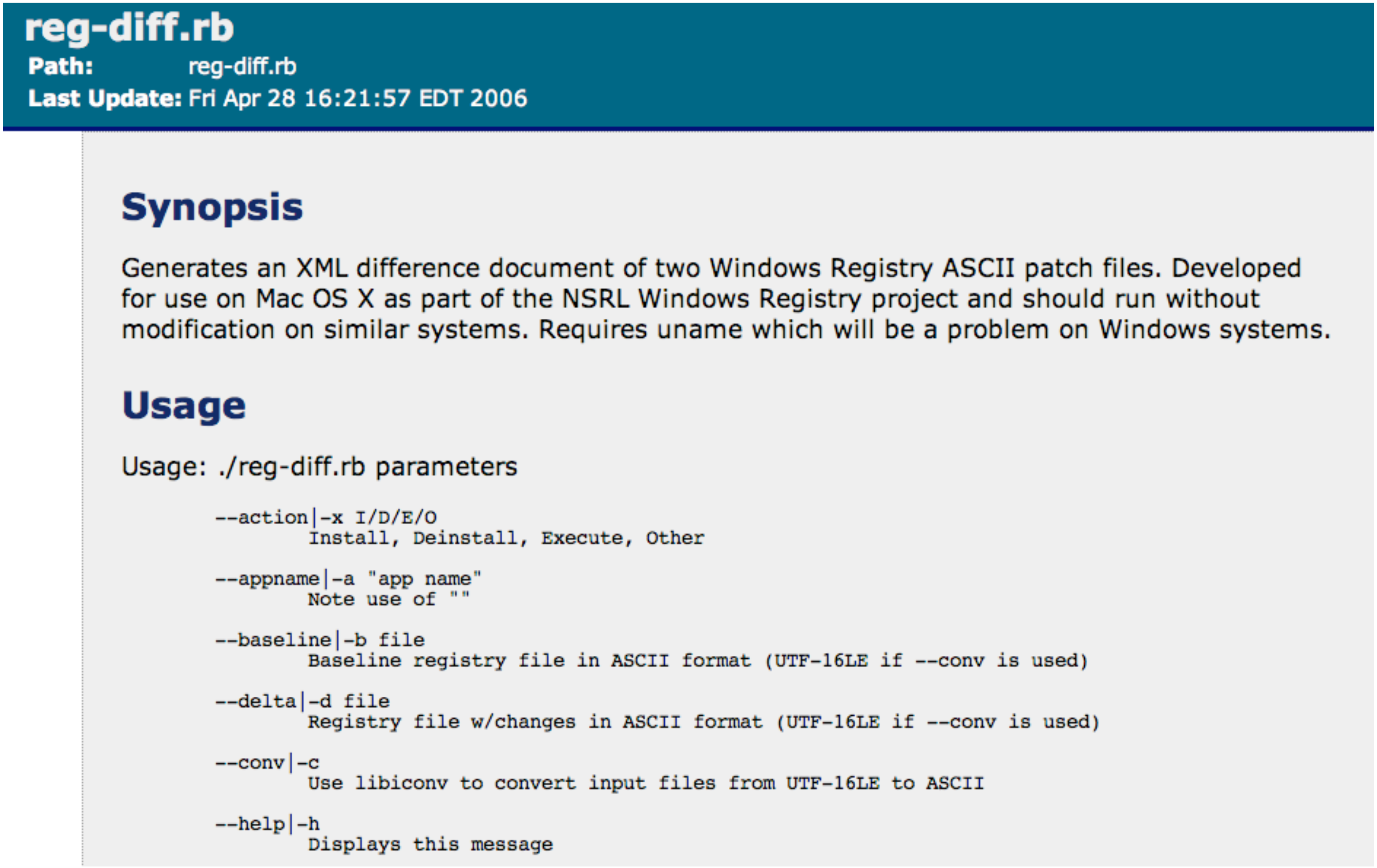
Synopsis

Generates the WIRED dataset from WIRED Difference Files in XML format.

Usage

Usage: ./mk-dataset.rb parameters file …

```
--action|-x A|O (default = A)
        Action to perform relative to output - add/overwrite

--debug|-d
        Generate extra columns in output file for debugging purposes

--help|-h
        Displays this message

--no-headers|-n
        Don't put column headers at top of output file

--output|-o file
        ASCII Windows Registry Dataset file, stdout is default

--verbose|-v
        Verbose mode
```



reg-diff.rb

Path: reg-diff.rb

Last Update: Fri Apr 28 16:21:57 EDT 2006

Synopsis

Generates an XML difference document of two Windows Registry ASCII patch files. Developed for use on Mac OS X as part of the NSRL Windows Registry project and should run without modification on similar systems. Requires uname which will be a problem on Windows systems.

Usage

Usage: ./reg-diff.rb parameters

```
        --action|-x I/D/E/O
                Install, Deinstall, Execute, Other

        --appname|-a "app name"
                Note use of ""

        --baseline|-b file
                Baseline registry file in ASCII format (UTF-16LE if --conv is used)

        --delta|-d file
                Registry file w/changes in ASCII format (UTF-16LE if --conv is used)

        --conv|-c
                Use libiconv to convert input files from UTF-16LE to ASCII

        --help|-h
                Displays this message
```

Contents

The WiReD dataset currently has the following fields:

- CHANGE_TYPE - if the Registry entry was added, deleted or modified
- APP_NAME - the application's name
- NSRL_APP_ID - if the application is part of the NSRL, its ID
- ACTION - whether the application was installed, deinstalled, executed or some other type of registry modification occurred
- ENTRY_TYPE - is the Registry entry a key or value?
- PATH - the Registry entry's path
- VALUE_NAME - if the entry is a value, its name
- VALUE_DATA - if the entry is a value, the data it contains

Example Data

```
add      1-2-3 Click n Submit Software Setup                    I       value
   HKEY_USERS\S-1-5-21-2170371235-572454927-963639892-
   1004\Software\Microsoft\Windows\ShellNoRoam\MUICache
   @C:\\PROGRA~1\\MSNGAM~1\\Windows\\rvseres.dll,-1212
   "Internet Reversi"
add      1-2-3 Click n Submit Software Setup                    I       value
   HKEY_USERS\S-1-5-21-2170371235-572454927-963639892-
   1004\Software\Microsoft\Windows\ShellNoRoam\MUICache
   @C:\\WINDOWS\\inf\\unregmp2.exe,-4   "Windows Media Player"
add      1-2-3 Click n Submit Software Setup                    I       value
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
   Uninstall\1-2-3 Click n Submit Softwares_is1       Inno Setup: User  "Alden
   Dima"
add      1-2-3 Click n Submit Software Setup                    I       value
   HKEY_USERS\S-1-5-21-2170371235-572454927-963639892-
   1004\Software\Microsoft\Windows\ShellNoRoam\MUICache
   @shell32.dll,-22040    "Local Security Policy"
```

Continuing Efforts

Prioritization of identifying and acquiring software

Processing software is person-intensive; automation and virtualization are goals

The current prototype is seen as a step in a much larger scheme that includes an XML database

Expansion of Registry modification detection to include all phases of an application's life cycle

Publicly available, request feedback from LEOs

Contacts

Douglas White
www.nsrl.nist.gov
nsrl@nist.gov

Barbara Guttman
Software Diagnostics & Conformance Testing Division
barbara.guttman@nist.gov

Sue Ballou, Office of Law Enforcement Standards
Rep. For State/Local Law Enforcement
susan.ballou@nist.gov